**computer networks**

**PRACTICAL 2**

***submitted by***

**takoliya manav anilbhai (21BCE530)**

**B.TECH**

**in**

**COMPUTER SCIENCE AND ENGINEERING**

***Guided by***

**Dr. VIJAY UKANI**

**Logo

Description automatically generated**

**NIRMA INSTITUTE OF TECHNOLOGY AHMEDABAD**

**27 AUGUST 2022**

**PRACTICAL 2**

**Aim: Analyze ping command**

**Uses:**

1. Test network connectivity.
2. Test network interface card.
3. Test DNS name resolution issues.

**Steps:**

The first step in troubleshooting is to ensure you can ping locally. To do this:

1. Go to Start > Run, type CMD and press Enter.
2. Type ping 127.0.0.1 and press Enter.
3. If this fails, troubleshoot your firewall.

**If that step was successful:**

1. Type ping 25.x.x.x where 25.x.x.x is your own Hamachi IP.
2. If this fails, again revisit your firewall settings.

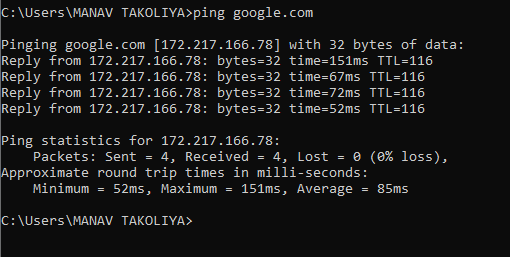
**If this was successful:**

1. Type ping 25.x.x.x where 25.x.x.x is the IP of the target computer.
2. If this fails, you'll need to troubleshoot the firewall on that machine

If you use IPv6 protocol mode, you need to type ping -6 <IPv6 address>. For example,

**ping -6 2620:9b::586:5b0c**

**Snapshot:**

****

**Observation:**

When we ping any server, our computer sends four data packets to the server. In reply, that server sends back those four data packets to us. This reply is called an "echo reply request."

If the server replies, then that means there is network connectivity between our computer and that server.

The server may be located on a local area network or on the internet.

If we did not get a reply from the server, then that means the server did not reply back, and it could mean that there is no connectivity between us and the server.

The cause of the server's failure to respond:

1.The server can be turned off.

2. The server is secured by a firewall.

3. "Destination host unreachable" means the route of destination could not be found.

The cause of getting the data packet 4:

1.NETWORK CONGESTION

2. Faulty Hardware (such as an incorrect Ethernet cable, wiring, modem, or network card)

We can also do a loopback test on our computer to check if our network card is working properly or not.

We have two options for that.

1. ping localhost ( loopback address)

2. 127.0.0.1 ( loopback address)



What is a byte: The size of the packet we send to the server is -32 bytes. 32 is the default size in Windows.

What is time : This indincate round trip time,time take be HOST A to HOST B and back to HOST A .

What is TTL : Time to live (TTL) refers to the amount of time or “hops” that a packet is set to exist inside a network before being discarded by a router.

**Aim: Analyze tracert command**

Tracert sends 3 data packets to every router and sends round trip time accordingly.

**Uses:**

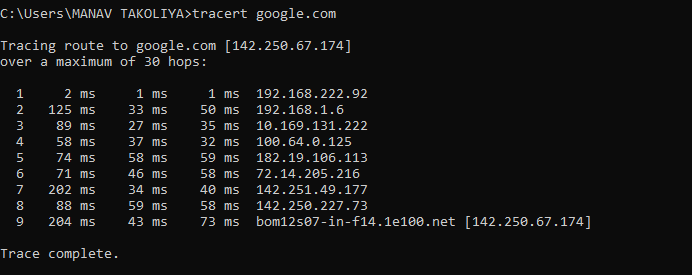
1. used to show a data packet's path from source to destination.

2. Traceroute can help you find problems like bottlenecks (from where our network is lagging)

**Steps:**

1. Press Windows key + R to open the Run window.
2. Enter cmd and press Enter to open a Command Prompt.
3. Enter tracert, a space, then the IP address or web address for the destination site (for example: tracert www.lexis.com).
4. Press Enter.

**Snapshot:**



**Observation:**

1. 1's column tells us about the hops taken by data packet. In our example, it is 9 hopes.

2. The next 3 columns tell us about the round trip of our data packets from each router to our computer.

3. The last column tells us the IP address of each router and its final destination.

4. \* means There is a problem with the router, or it may be possible that the router is working fine but it was not configured to return traceroute replies.

5. Maximum of 30 hops means TTL sets a maximum of 30 hops which means if a data packet does not reach its destination after 30 hops, then it will be dropped.

-We can change maximum hops.

      tarcert -h 4 google.com

What is use of TTL:

TTL prevent data packets from travelling endless around the internet.

**Aim:- Analyze of nslookup**

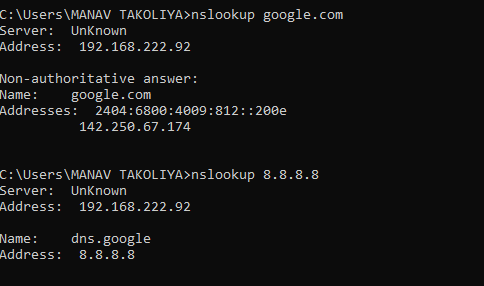
**USE:**

Getting information from the DNS server

**Steps:**

1. Launch Windows Command Prompt by navigating to Start > Command Prompt or via Run > CMD.
2. Type NSLOOKUP and hit Enter. ...
3. Set the DNS Record type you wish to lookup by typing set type=## where ## is the record type, then hit Enter.

**Snapshot:**

****

**Observation :**

1. **It resolves the name of the DNS server and it also resolves or configures the IP address.**
2. nslookup is a simple but very practical command-line tool, which is principally used to find the **IP address** that corresponds to a host, or the domain name that corresponds to an IP address (a process called “Reverse DNS Lookup”).

**Aim: Analyze ipconfig command**

**Use:**

It displays the TCP/IP network configuration of the network adapters on a Windows computer.

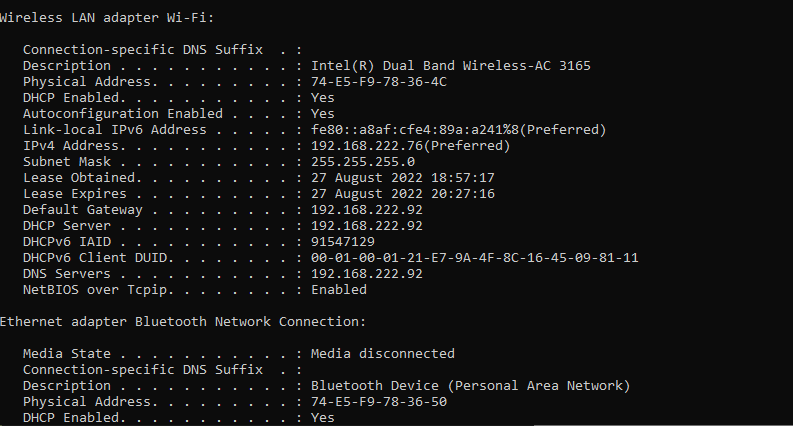
used for troubleshooting issues.

Steps:

Go to "Start > Run" and type “cmd” (no quotes), then select "OK"

Type "ipconfig/release" (no quotes) and press "Enter"

Snapshot :



**Observation:**

IPCONFIG displays things like IP addresses,subnet masks, and the default gateway.

1.IPv4 is the private IP address that has been assigned to us by the DHCP server. That's built into our router and modem/router combo that's in our home and office .

2. Default Gateway: This is the IP address of your home's router or modem/router combo that connects to your network. which allows you to communicate with different networks.

3.We have assigned IPv4 and IPv6 addresses.

4. The ipconfig/all command displays your network adapters' complete TCP/IP configuration.

5. The ipconfig/flushdns command clears the computer's DNS resolver cache.

6. Because the computer only understands numbers and not the name of the site, we must convert the name into an IP address.

7. DNS resolver cache stores a history of domain names and their corresponding IP addresses for a period of time.The purpose of this is to make the browser fast.

8. When can we use ipconfig /flushdns: We can use this command when we cant access some site.

9. When can we use ipconfig/flushdns?  We can use this command when we can't access some site.

**Aim: Analyze netstat -r command**

**Use:**

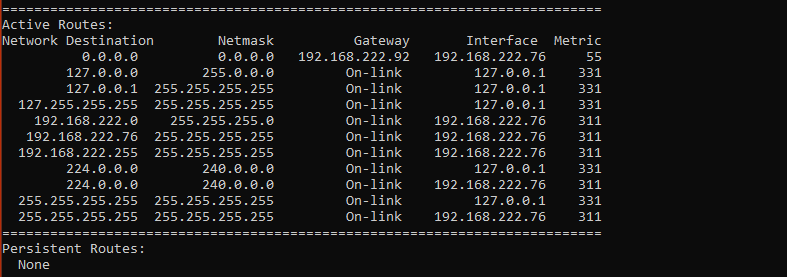
to display current network connectivity and port activity on your computer.

Available on various operating systems,

**Steps:**

1. Launch Windows Command Prompt by navigating to Start > Command Prompt or via Run > CMD.
2. Type netstat -options and hit Enter. ...

**Snapshot:**



Observation:

1. netstat -n returns the IP address instead of the domain name.

2. netstat -a displays TCP and UDP ports

3. netstat -b displays the protocol along with the application name.

4. netstat -f displays the domain name rather than the IP address in foreign addresses.

5. netstat -r display the routing table

We can combine all these switches (attributes).

**Aim: Analyze arp -a command**

**Use:**

Displays and modifies address resolution, including ATM (Asynchronous Transfer Mode) interfaces.

It is used to convert IP addresses to Mac addresses.

Devices need the mac address for communication on the local network.

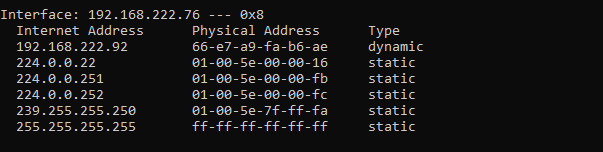
Use arp to acquire a mac address for that device.

**-a : To Display ARP Entries**

**Steps :**

1. Open cmd
2. Type arp – a and hit enter

**Snapshot:**



**Observation :**

How it works:-

Our computer sends a request for the mac address of a network device. A correspondent device on the network will respond to it by sending its mac address.

Now our computers store the IP address and Mac address of that computer in the arp cache.

An ARP cache is used to make a network more efficient.

Arp entries are classified into two types:

1.static : The static entry is where someone mannually enters an IP to MAC address association using the ARP command line utility.

2. dynamic: it is generated automatically when a device broadcasts a message over the network.